Pentagon Launches Two—Week Cyber Review After Microsoft Ends China—Based Support

July 19, 2025
— Categories: Defence & Security

The U.S. Department of Defense has initiated a two-week review of its digital infrastructure after Microsoft confirmed it had stopped using China-based engineering teams to support its sensitive defense cloud services. The decision highlights rising concern over foreign involvement in national security-related technology.

Microsoft's Chief Communications Officer, Frank Shaw, stated that the company had already ceased employing China-based engineers for Department of Defense (DoD) cloud support. This follows a recent investigation that revealed that foreign-based teams had access to critical U.S. systems with limited oversight, sparking alarms over cybersecurity vulnerabilities.

Defense Secretary Pete Hegseth acknowledged that the systems involved were part of a "legacy" setup inherited from a previous administration. He has ordered a thorough two-week review, if not sooner, to ensure that similar risks do not exist elsewhere within military networks. The review aims to uncover and correct any weaknesses in cybersecurity protocols tied to foreign contractors or offshored technical support.

The Pentagon's response demonstrates a heightened sense of urgency in safeguarding the nation's military infrastructure from potential cyber threats. Hegseth pledged that further actions would be taken if needed, reaffirming the department's commitment to ensuring defense systems are, in his words, "ironclad and impenetrable."

The situation drew swift reaction from lawmakers, including Senator Tom Cotton, who cited the report as a clear example of how foreign access can compromise national security. He and others are urging additional scrutiny into how third-party tech vendors handle sensitive government data.

Microsoft has pledged to continue working with national security partners to enhance cloud security and prevent similar risks going forward. Shaw reiterated the company's commitment to upholding high standards when

servicing U.S. government clients, particularly in defense-related operations.

This review represents a broader reckoning within the Pentagon as it reassesses how deeply foreign engineering support is embedded in critical defense systems. The findings may influence future policy by limiting or prohibiting overseas personnel from working on sensitive military technologies, even indirectly.

As the Department of Defense moves swiftly to address potential lapses, the episode serves as a cautionary example of the geopolitical risks attached to modern, globally outsourced technology ecosystems.